

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-338868
 (43)Date of publication of application : 08.12.2000

(51)Int.Cl. G09C 1/00
 H04L 9/08
 H04L 9/10
 H04L 9/32

(21)Application number : 11-146311
 (22)Date of filing : 26.05.1999

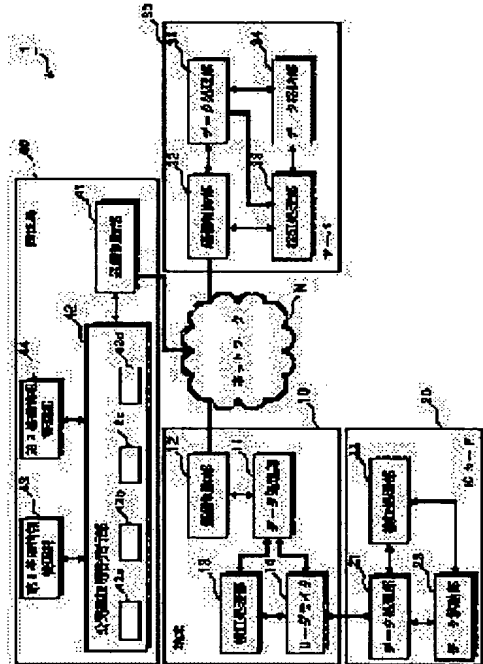
(71)Applicant : NTT DATA CORP
 (72)Inventor : TAKAHASHI YOSHIO
 TSUCHIYA SHIGEKI

(54) METHOD FOR ISSUING PUBLIC KEY CERTIFICATE, METHOD FOR VERIFYING, SYSTEM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a system which can issue and verify a public key certificate capable of dealing with to a plurality of formats.

SOLUTION: A verification office 40 generates signature data for EMV use objecting fundamental information for the EMV use when receiving information applying an issue of a public key certificate. Also, it generates the signature data for X 509 use objecting information containing the fundamental information for the EMV use and the signature data for the EMV use. It issues the X 509 public key certificate containing all of the generated information and data. This X 509 public key certificate is converted into the EMV public key certificate at a terminal 10 in order to be able to use with an IC card 20.



LEGAL STATUS

[Date of request for examination] 08.11.2000
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-338868

(P2000-338868A)

(43) 公開日 平成12年12月8日 (2000.12.8)

(51) Int.Cl. ⁷	識別記号	F I	ターコード* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
	6 3 0		6 3 0 F
	6 6 0		6 6 0 A
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 F
9/10			6 2 1 A
審査請求 未請求 請求項の数12 O L (全 12 頁) 最終頁に続く			

(21) 出願番号 特願平11-146311
(22) 出願日 平成11年5月26日 (1999.5.26)

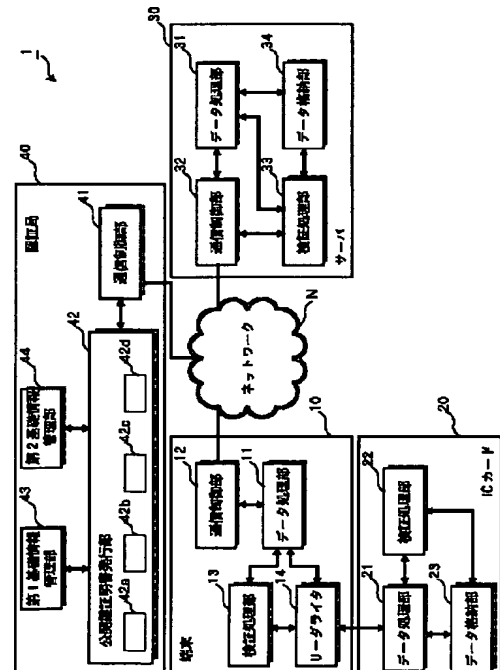
(71) 出願人 000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(72) 発明者 高橋 芳夫
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(72) 発明者 土屋 茂樹
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(74) 代理人 100099324
弁理士 鈴木 正剛
Fターム(参考) 5J104 AA09 AA16 EA05 JA21 LA03
LA06 MA02 NA12 NA35 PA07

(54) 【発明の名称】 公開鍵証明書発行方法、検証方法、システム及び記録媒体

(57) 【要約】

【課題】 複数のフォーマットに対応可能な公開鍵証明書を発行し、検証できるシステムを提供する。

【解決手段】 認証局40は、公開鍵証明書の発行申請情報を受け取ると、EMV用の基礎情報を対象としたEMV用の署名データを生成する。また、EMV用の基礎情報とEMV用の署名データを含む情報を対象としたX509用の署名データを生成する。上記生成した情報及びデータをすべて含んだX509公開鍵証明書を発行する。このX509公開鍵証明書は、ICカード20で使用するようにするため、端末10でEMV公開鍵証明書に変換する。



【特許請求の範囲】

【請求項 1】 所定の申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報のうち、一のフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成するとともに、

前記生成した基礎情報及び署名データと他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する過程を含む、
公開鍵証明書の発行方法。

【請求項 2】 請求項 1 記載の発行方法において作成された公開鍵証明書から前記一のフォーマット用の基礎情報、前記一のフォーマット用の署名データ、前記他のフォーマット用の基礎情報、前記他のフォーマット用の署名データを取得し、取得した情報及び署名データに基づいて前記一のフォーマット用の公開鍵証明書を作成する過程を含む、

公開鍵証明書の発行方法。

【請求項 3】 請求項 1 又は 2 記載の発行方法により発行された公開鍵証明書から前記各基礎情報及び署名データを取り出して当該公開鍵証明書の正当性を検証する装置において実行される方法であって、

前記取り出した各基礎情報をそれが対応するフォーマット以外の他のフォーマットに変換することで当該他のフォーマットに対応する基礎情報を生成し、前記公開鍵証明書から取り出した基礎情報又は前記他のフォーマットに対応する基礎情報と前記公開鍵証明書から取り出した複数の署名データのいずれかが合致する場合に、前記公開鍵証明書を正当と判断することを特徴とする、

公開鍵証明書の検証方法。

【請求項 4】 所定の申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報をすべてのフォーマットに共通の基礎情報と各フォーマットに固有の基礎情報とに分類する基礎情報生成手段と、

前記共通の基礎情報及び一のフォーマットに固有の基礎情報を対象とした当該一のフォーマット用の署名データを生成する署名手段と、

前記生成した基礎情報及び署名データと、他のフォーマットに固有の基礎情報と、前記一のフォーマット及び他のフォーマットに共通の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する発行手段とを有し、一のフォーマットと他のフォーマットのいずれにも対応可能な公開鍵証明書を発行することを特徴とする、

公開鍵証明書発行装置。

【請求項 5】 所定の申請情報に基づいて複数フォーマットに対応可能な公開鍵証明書を発行する第 1 装置と、発行された公開鍵証明書を独自フォーマットの公開鍵証明書に変換する第 2 装置とを有し、

第 1 装置は、

前記申請情報に基づいて生成された公開鍵証明書用の複数の基礎情報をすべてのフォーマットに共通の基礎情報と各フォーマットに固有の基礎情報に分類する基礎情報生成手段と、

前記共通の基礎情報及び一のフォーマットに固有の基礎情報を対象とした当該一のフォーマット用の署名データを生成する署名手段と、

前記生成した基礎情報及び署名データと、他のフォーマットに固有の基礎情報と、前記一のフォーマット及び他のフォーマットに共通の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する公開鍵証明書発行手段とを有し、

第 2 装置は、

前記他のフォーマット用の公開鍵証明書から前記共通の基礎情報、前記一のフォーマットに固有の基礎情報、前記一のフォーマット用の署名データ、前記他のフォーマットに固有の基礎情報及び前記他のフォーマット用の署名データを取得し、取得した情報及びデータに基づいて前記一のフォーマット用の公開鍵証明書を作成する手段を有することを特徴とする、
公開鍵証明書発行システム。

【請求項 6】 第 2 装置は、前記一のフォーマット用の公開鍵証明書を検証した後、その公開鍵証明書を所定の情報記録媒体に格納するように構成されていることを特徴とする、請求項 5 記載の公開鍵証明書発行システム。

【請求項 7】 第 1 装置及び第 2 装置の少なくとも一方が、ネットワークに接続されたプロキシ装置で構成されていることを特徴とする、

30 請求項 5 記載の公開鍵証明書発行システム。

【請求項 8】 所定の申請情報に基づいて生成された公開鍵証明書用の複数のフォーマットの基礎情報を所定順に配列するとともに、各基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成し、

申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、前記生成された署名データとを含めて公開鍵証明書を作成する過程を含む、
公開鍵証明書の発行方法。

【請求項 9】 請求項 8 記載の発行方法により発行された公開鍵証明書から前記基礎情報、前記複数のハッシュ値及び署名データを取り出す過程と、

取り出した基礎情報をハッシュしてハッシュ値を生成するとともに、生成したハッシュ値と前記公開鍵証明書から取り出したハッシュ値とを連結して連結ハッシュ値を生成する過程と、

生成した連結ハッシュ値と前記公開鍵証明書から取り出した署名データとを比較する過程とを含み、

署名データと連結ハッシュ値とが合致する場合に前記公開鍵証明書を正当と判断することを特徴とする、公開鍵証明書の検証方法。

【請求項 10】 所定の申請情報に基づいて生成された公開鍵証明書の複数のフォーマットの基礎情報を所定順に配列する基礎情報配列手段と、複数の基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する署名手段と、申請者側で利用可能なフォーマットに対応する基礎情報、該フォーマットに対応する基礎情報以外の基礎情報から生成したハッシュ値及び前記生成した署名データを含めて公開鍵証明書を作成する発行手段とを有し、複数のフォーマットに対応可能な一つの公開鍵証明書を発行することを特徴とする、公開鍵証明書発行装置。

【請求項 11】 所定の申請情報に基づいて公開鍵証明書の複数の基礎情報を用意する処理、前記複数の基礎情報のうちのフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成する処理、前記生成した基礎情報及び署名データと他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて前記他のフォーマット用の公開鍵証明書を作成する処理をコンピュータに実行させるためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【請求項 12】 所定の申請情報に基づいて公開鍵証明書の複数のフォーマットの基礎情報を生成する処理、前記複数のフォーマットの基礎情報の各々ハッシュ値を生成する処理、生成された複数のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する処理、申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、前記生成された署名データとを含めて公開鍵証明書を作成する処理をコンピュータに実行させるためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、汎用のメディア用の標準のフォーマットとリソースの小さなメディアに適した独自のフォーマットのいずれにも対応可能な公開鍵証明書を発行する技術、及び発行された公開鍵証明書の検証技術に関する。メディアとは公開鍵証明書を利用する情報処理手段（端末、ICカード等）であり、フォーマットとは、メディアが解釈可能な公開鍵証明書の規格をいう。

【発明の詳細な説明】

【0002】

【発明の背景】 近年、電子メールシステム、電子マネー

システム、電子決済システム、電子商取引システム、電子申請システム等のネットワークを利用した様々なシステムが実用化されている。このようなシステムでは通信の秘匿性が非常に重要になることから暗号化技術が応用されているが、現在は、暗号鍵や復号鍵を保守するにあたっての労力が小さくて済むという利点を持つ公開鍵暗号方式が広く用いられるようになっている。

【0003】 公開鍵暗号方式では、その公開鍵の持ち主を証明するために、公共性の強い認証局と呼ばれる機関が認証局による署名データ入りの公開鍵証明書を発行するのが一般的である。公開鍵証明書には、多種多様な目的や用途に対して柔軟に対応することがその性質上求められているが、従来は、そのフォーマットに様々な項目を含めることによってその汎用性を確保している。例えば、公開鍵証明書の標準となっている ITU-T（国際電気通信連合電気通信標準化部門）の「X509」は、非常に多くの項目を含んでおり、その内容がかなり複雑なものとなっている。このような複雑な内容の公開鍵証明書は、その汎用性ゆえに非常に魅力的なものとなっているが、その反面、これを IC カード等のようなリソースの少ないものに応用する場合は難点がある。

【0004】 即ち、リソースの小さい IC カード等では、汎用性の高い上記のような一般的な公開鍵証明書を取り扱うには、プログラムサイズの増大、処理時間の増加、メモリの圧迫といった問題が発生し、そのまま利用できない場合が生じる。このような場合には、特定サービス限定の独自フォーマットを採用することが考えられるが、そのためには、汎用性のある公開鍵証明書のインフラ以外の専用インフラを構築することが必要となるが、これは、その手間やコストの面から見て必ずしも妥当な解決手段とはいえない。

【0005】 もし、IC カード等のリソースの小さなものに、ITU-T「X509」等の汎用性の高いフォーマットを採用した場合、或いは IC カード内部で汎用フォーマットを独自フォーマットに変換し、これを保管することにした場合、上記のような難点を理論上は解消できるが、IC カードの限られたリソースが、フォーマットの解釈や変換機能を実現するために消費されてしまい、そもそも実装できないか、本来達成しようとしていた機能を十分に達成できない事態が生じる。

【0006】 本発明は、標準のフォーマットにも対応することができ、且つリソースの小さなメディアでの使用にも適した汎用性の高い公開鍵証明書の発行方法、発行装置、発行システムを提供することをその主たる課題とするものである。本発明は、また、公開鍵証明書の検証を適切に行うことができる検証方法及び、公開鍵証明書の発行方法を汎用のコンピュータ上で実現する上で好適となる記録媒体を提供することをその課題とする。

【0007】

【課題を解決するための手段】 本発明は、上記課題を解

決するために以下に説明するような2通りの公開鍵証明書
の発行方法を提供する。第1の公開鍵証明書の発行方
法は、所定の申請情報に基づいて生成された公開鍵証明
書用の複数の基礎情報のうち、一のフォーマット用の基
礎情報を対象とした当該一のフォーマット用の署名デー
タを生成するとともに、前記生成した基礎情報及び署名
データと、他のフォーマット用の基礎情報とを対象とし
た当該他のフォーマット用の署名データを含めて前記他
のフォーマット用の公開鍵証明書を作成する。また、作
成された公開鍵証明書から前記一のフォーマット用の基
礎情報、前記一のフォーマット用の署名データ、前記他
のフォーマット用の基礎情報、前記他のフォーマット用
の署名データを取得し、取得した情報及び署名データに
基づいて前記一のフォーマット用の公開鍵証明書を作成
する。このような過程を含む公開鍵証明書の発行方法で
ある。

【0008】この方法により発行された公開鍵証明書
は、以下のようにして検証することができる。まず、公
開鍵証明書から各基礎情報及び署名データを取り出し、
必要な場合に、取り出した各基礎情報をそれが対応する
フォーマット以外の他のフォーマットに変換することで
当該他のフォーマットに対応する基礎情報を生成し、公
開鍵証明書から取り出した基礎情報又は前記他のフォー
マットに対応する基礎情報と公開鍵証明書から取り出し
た複数の署名データのいずれかが合致する場合に、そ
の公開鍵証明書を正当と判断する。

【0009】フォーマットの変換を行った場合は、基礎
情報と署名データとの間における照合を行えなくなるの
が通常である。しかしながら、この発明で発行される公
開鍵証明書には、複数の署名データが含まれており、且
つこの署名データは、他のフォーマットに変換した基礎
情報を署名対象として生成されているので、フォーマッ
ト変換後においても照合が可能になる。また、フォーマ
ット変換を前提とすることにより、特定サービス/アプ
リケーションに最適化した基礎情報のフォーマットを採
用しても、独自フォーマット専用のインフラを構築する
必要がなくなる。

【0010】上記の公開鍵証明書の発行方法は、例え
ば、以下のように構成される公開鍵証明書発行装置又は
システムによってその実行が可能である。公開鍵証明書
発行装置は、所定の申請情報に基づいて生成された公開
鍵証明書用の複数の基礎情報をすべてのフォーマットに
共通の基礎情報と各フォーマットに固有の基礎情報とに
分類する基礎情報生成手段と、前記共通の基礎情報及び
一のフォーマットに固有の基礎情報を対象とした当該一
のフォーマット用の署名データを生成する署名手段とを
有し、さらに、生成した基礎情報及び署名データ、他の
フォーマットに固有の基礎情報、一のフォーマット及び
他のフォーマットに共通の基礎情報とを対象とした当該
他のフォーマット用の署名データを含めて他のフォーマ

ット用の公開鍵証明書を作成する発行手段とを有し、一
のフォーマットと他のフォーマットのいずれにも対応可
能な公開鍵証明書を発行する装置である。

【0011】公開鍵証明書発行システムは、所定の申請
情報に基づいて複数フォーマットに対応可能な公開鍵証
明書を発行する第1装置と、発行された公開鍵証明書を
独自フォーマットの公開鍵証明書に変換する第2装置と
を含んで構成される。第1装置は、申請情報に基づいて
生成された公開鍵証明書用の複数の基礎情報をすべての
フォーマットに共通の基礎情報と各フォーマットに固有
の基礎情報に分類する基礎情報生成手段と、前記共通の
基礎情報及び一のフォーマットに固有の基礎情報を対象
とした当該一のフォーマット用の署名データを生成する
署名手段と、生成した基礎情報及び署名データと他のフ
ォーマットに固有の基礎情報と一のフォーマット及び他
のフォーマットに共通の基礎情報とを対象とした当該他
のフォーマット用の署名データを含めて他のフォーマッ
ト用の公開鍵証明書を作成する公開鍵証明書発行手段と
を有するものであり、第2装置は、他のフォーマット用
の公開鍵証明書から共通の基礎情報、一のフォーマット
に固有の基礎情報、一のフォーマット用の署名データ、
他のフォーマットに固有の基礎情報及び他のフォーマッ
ト用の署名データを取得し、取得した情報及びデータに
基づいて一のフォーマット用の公開鍵証明書を作成する
手段を有するものである。第2装置は、例えば、一のフ
ォーマット用の公開鍵証明書を検証した後、その公開鍵
証明書を所定の情報記録媒体に格納するように構成され
る。なお、第1装置及び第2装置は、例えばネットワー
クを介して接続された独立の装置であっても良く、第1
装置及び第2装置の少なくとも一方の機能を同一の情報
処理装置又はシステム内で構築しても良い。後者の場
合、その情報処理装置又はシステムをプロキシ (prox
y) 装置とすることで、外部に隠蔽された状態で本発明
の公開鍵証明書発行方法を実現することができる。ま
た、このプロキシ装置に、既存の公開鍵発行システムに
ない部分のみを配置し、既存の公開鍵発行システムと共
同で公開鍵証明書を発行するようにすることで、本発明
の実施がより容易となる。

【0012】次に、第2の公開鍵証明書の発行方法につ
いて説明する。この方法は、所定の申請情報に基づいて
生成された公開鍵証明書用の複数のフォーマットの基礎
情報を所定順に配列するとともに、各基礎情報の各々の
ハッシュ値を連結した連結ハッシュ値を対象として署名
データを生成し、申請者側で利用可能なフォーマットに
対応する基礎情報と、この基礎情報のフォーマット以外
の他のフォーマットの基礎情報から生成したハッシュ値
と、生成された署名データとを含めて公開鍵証明書を作
成する過程を含む方法である。ハッシュ値の連結は、複
数のハッシュ値の論理条件を判定することにより行う。
第1の公開鍵証明書発行方法と比較して第2の公開鍵証

明書の発行方法は、それにより得られる公開鍵証明書のデータ量を小さくすることができる。これは、ハッシュ値のデータ量が、署名データのデータ量よりも小さいことに基く。

【0013】この発行方法により発行された公開鍵証明書の検証は、以下のようにして行われる。即ち、検証を行う装置において、公開鍵証明書から基礎情報、複数のハッシュ値及び署名データを取り出す過程と、取り出した基礎情報をハッシュしてハッシュ値を生成するとともに、生成したハッシュ値と前記公開鍵証明書から取り出したハッシュ値とを連結して連結ハッシュ値を生成する過程と、生成した連結ハッシュ値と前記公開鍵証明書から取り出した署名データとを比較する過程とをこの順に実行し、署名データと連結ハッシュ値とが合致する場合に公開鍵証明書を正当と判断する。

【0014】第2の公開鍵証明書の発行方法は、例えば以下のような公開鍵証明書発行装置において実施することができる。この公開鍵証明書発行装置は、所定の申請情報に基づいて生成された公開鍵証明書の複数のフォーマットの基礎情報を所定順に配列する基礎情報配列手段と、複数の基礎情報の各々のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する署名手段と、申請者側で利用可能なフォーマットに対応する基礎情報、該フォーマットに対応する基礎情報以外の基礎情報から生成したハッシュ値及び生成した署名データを含めて公開鍵証明書を作成する発行手段とを有し、複数のフォーマットに対応可能な一つの公開鍵証明書を発行することを特徴とするものである。

【0015】第1及び第2の公開鍵証明書の発行方法を汎用のコンピュータ上で実行する上で用いる記録媒体は、それぞれ以下のようなものである。第1の公開鍵証明書の発行方法をコンピュータ上で実現するための記録媒体は、コンピュータに下記の処理を実行させるためのプログラムが記録されたコンピュータ読みとり可能な記録媒体である。

(1-1) 所定の申請情報に基づいて公開鍵証明書の複数の基礎情報を用意する処理、(1-2) 前記複数の基礎情報のうちのフォーマット用の基礎情報を対象とした当該一のフォーマット用の署名データを生成する処理、(1-3) 生成した基礎情報及び署名データと、他のフォーマット用の基礎情報とを対象とした当該他のフォーマット用の署名データを含めて他のフォーマット用の公開鍵証明書を作成する処理。

【0016】第2の公開鍵証明書の発行方法をコンピュータ上で実現するための記録媒体は、コンピュータに下記の処理を実行させるためのプログラムが記録されたコンピュータ読みとり可能な記録媒体である。

(2-1) 所定の申請情報に基づいて公開鍵証明書の複数のフォーマットの基礎情報を生成する処理、(2-2) 複数のフォーマットの基礎情報の各々ハッシュ値を

生成する処理、(2-3) 生成された複数のハッシュ値を連結した連結ハッシュ値を対象として署名データを生成する処理、(2-4) 申請者側で利用可能なフォーマットに対応する基礎情報と、この基礎情報のフォーマット以外の他のフォーマットの基礎情報から生成したハッシュ値と、前記生成された署名データとを含めて公開鍵証明書を作成する処理。

【0017】

【発明の実施の形態】以下、図面を参照して、本発明による公開鍵証明書発行方法、検証方法、発行システムの実施の形態を説明する。ここでは、標準フォーマットであるITU-T「X509」と、リソースの小さなICカード用の単純なフォーマット「EMV」との間の互換が可能な公開鍵証明書の例を挙げる。

【0018】(第1実施形態) まず、第1の公開鍵証明書発行方法の実施の形態を説明する。図1は、この方法の実施に適した公開鍵証明書サービスシステムの構成図である。この公開鍵証明書サービスシステム1は、フォーマットの互換性を有する公開鍵証明書を発行する機能を有する認証局40、上記公開鍵証明書を独自フォーマットの公開鍵証明書に変換する機能を有する端末10、端末10によってフォーマット変換された公開鍵証明書を保持するとともにサーバ30の公開鍵証明書の検証機能を有するICカード20、ICカード20の公開鍵証明書の検証機能を有するサーバ30を、それぞれ双方向通信可能な環境のネットワークNに接続して構成される。

【0019】端末10は、ICカード20との間で情報の授受を行うリーダライタ14を有する一種のコンピュータである。この端末10は、図示しないコンピュータのCPUが自己のオペレーティングシステム下で所定のプログラムを読み込んで実行することにより形成されるデータ処理部11、通信制御部12、及び検証処理部13とを含んで構成される。データ処理部11は、ICカード20等との間でデータのやりとりを行ったり所定の変換アルゴリズムに従って公開鍵証明書のフォーマット変換等を行うものであり、通信制御部12は、ネットワークを経由する情報の制御を行うものである。検証処理部13は、公開鍵証明書等の検証を行うものである。

【0020】ICカード20は、端末10等との間でデータのやりとりを行うデータ処理部21、公開鍵証明書の検証を行う検証処理部22、及び自己の公開鍵証明書や検証済みの公開鍵等を格納するデータ格納部23を含んで構成される。これらのデータ処理部21、検証処理部22、データ格納部23は、図示しないROM内のプログラムをCPUが実行することにより形成される。

【0021】サーバ30は、端末10や認証局40との間でデータのやりとりを行うデータ処理部31、ネットワークNからの情報を制御する通信制御部32、公開鍵証明書の検証を行う検証処理部33、及び検証した公開鍵証明書や公開鍵等を格納するデータ格納部34を含ん

で構成されている。

【0022】認証局40は、コンピュータないしコンピュータシステムによって実現されるもので、コンピュータ等のCPUが自己のオペレーティングシステム下で所定のプログラムを読み込んで実行することにより形成される各種機能ブロック、即ち、ネットワークNからの情報を制御する通信制御部41、公開鍵証明書の発行や生成を管理する公開鍵証明書発行部42、各々異なるフォーマットの基礎情報を管理する第1基礎情報管理部43及び第2基礎情報管理部44を含んで構成されている。公開鍵証明書発行部42は、申請者からの申請情報に基づいて公開鍵証明書用の基礎情報を生成する基礎情報生成部42aと、基礎情報を対象とした署名データを生成する署名部42bと、基礎情報及び署名データを含めて公開鍵証明書を作成（発行）する発行部42cとを含んでいる。

【0023】次に、上記のように構成される公開鍵証明書サービスシステムの動作を説明する。まず、認証局40において公開鍵証明書を発行する場合の手順を図2を参照して説明する。ここでは、あとでICカード20用のEMVフォーマットに変換されることを考慮したX509フォーマットの公開鍵証明書を発行するものとする。以後の説明では、フォーマットの種類を区別する必要がある場合において、X509フォーマットを「X509」、EMVフォーマットを「EMV」と表現する。また、各フォーマットの公開鍵証明書に記述すべき項目のうち、X509とEMVに共通の項目をC、X509のみに必要な項目をA、EMVのみに必要な項目をBとする。

【0024】認証局40の公開鍵証明書発行部42は、例えば端末10から公開鍵証明書の申請情報を受け取ると（ステップS101）、この申請情報に基づいてX509、EMVに対応する項目（A、B、C）を作成ないし分類し、第2基礎情報管理部44に、項目C及び項目Bを対象としたEMV用の署名データSIGN#2を生成させる（ステップS102）。公開鍵証明書発行部42は、また、項目Bと上記署名データSIGN#2を公開鍵証明書の拡張領域に格納するデータ（「拡張データ」）APDX#2として、第1基礎情報管理部43に、項目C、項目A、及び拡張データAPDX#2を対象としたX509用の署名データSIGN#1を生成させる（ステップS103）。

【0025】その後、項目C、項目A、及びX509用の署名データSIGN#1を含んだX509公開鍵証明書を発行し（ステップS104）、これを通信制御部41を通して端末10宛に送付する。このようにして発行されたX509公開鍵証明書は、ICカード20において使用できるようにするため、端末10でEMV公開鍵証明書に変換される。具体的には、X509公開鍵証明書から項目C及び項目Bを取得してこれをEMVの基礎

情報DATA#2とする。また、拡張データAPDX#2からEMV用の署名データSIGN#2を取得し、さらに項目A及びX509用の署名データSIGN#1を取得してEMV公開鍵証明書に変換する。このようにして変換されたEMV公開鍵証明書は、端末10又はサーバ30で何時でもX509公開鍵証明書に変換できるようになっている。

【0026】図3は、X509公開鍵証明書とEMV公開鍵証明書の項目の対応関係を概念的に示した図である。認証局40から発行されたX509公開鍵証明書は、図3左側に示されるように、基本情報領域と基本署名領域とを有している。基本情報領域には、項目C、項目A、拡張データ（項目B及び署名データSIGN#2）APDX#2が格納される。これらの格納情報がX509用の基礎情報DATA#1となり、この基礎情報DATA#1を対象とした署名データSIGN#1が、基本署名領域に格納されるようになっている。

【0027】一方、EMV公開鍵証明書は、図右側に示されるように、その基本情報領域に、項目C及び項目Bのみが格納され、これらがEMV用の基礎情報DATA#2となる。そして、この基礎情報DATA#2を対象とした署名データSIGN#2が基本署名領域に格納されるようになっている。EMV公開鍵証明書の付属データ領域には、項目A及びX509用の署名データSIGN#1が、付属データAPDX#1として格納されるようになっている。

【0028】次に、各公開鍵証明書の検証処理について説明する。X509公開鍵証明書の検証処理は、X509用の署名データSIGN#1が基礎情報DATA#1についての正しい署名データになっているかどうかを確認する処理であり、EMV公開鍵証明書の検証処理は、EMV用の署名データSIGN#2が基礎情報DATA#2についての正しい署名データになっているかどうかを確認する処理である。

【0029】フォーマット変換を行った場合は署名データの照合を行えなくなるのが通常であるが、本実施形態の公開鍵証明書には、二種類のフォーマットによる署名データSIGN#1、SIGN#2が含まれており、しかもこれらの署名データのうち一方のフォーマットに対応するものは、他方のフォーマットに変換した基礎情報を署名対象として生成されたものとなっているので、フォーマット変換後においても照合等を行うことが可能になる。つまり、使用が予想されるフォーマットに変換した基礎情報を対象として生成した署名データを、複数の署名データの一つに含めて公開鍵証明書を作成しておけば、基礎情報とそれに基づいて作成された署名データとを照合することは、フォーマット変換後においても可能となる。

【0030】このように、本実施形態により発行される公開鍵証明書は、汎用性の高いX509フォーマット

と、ICカード20のようにリソースが小さいものにおいて利用し易いEMVフォーマットの両方に対応することができるので、フォーマット毎のインフラを別途構築する必要がなくなり、公開鍵証明書を利用するシステムの構成が簡略化される利点がある。

【0031】また、フォーマット変換を要する公開鍵証明書の検証処理は、リソースの大きな端末10が行い、ICカード20へは正当性が確認された公開鍵証明書を格納することで、ICカード20側で、フォーマット変換のために限られたリソースを無駄に使用することもなくなる。

【0032】以上、X509フォーマットとEMVフォーマットの両方に対応できる公開鍵証明書の発行、検証の例を示したが、一つの公開鍵証明書で3種類以上のフォーマットに対応できるようにすることも可能である。例えば図4は、4通りのフォーマット(フォーマット#1、フォーマット#2、フォーマット#3、フォーマット#4)に対応できるようにした公開鍵証明書の概念図である。基礎情報DATA#1から基礎情報DATA#4までの双方向のフォーマット変換は、リソースの大きなワークステーションで行い、リソースの小さいICカードでは、フォーマットの内容チェックやフォーマット変換を要しない検証のみを行う。

【0033】図4のように4通りのフォーマットに対応させる場合、ある一つのフォーマット、例えばフォーマット#1における基礎情報DATA#1とこの基礎情報DATA#1を他のフォーマットに変換した基礎情報(DATA#2、DATA#3、DATA#4)について生成した署名データを計4個(SIGN#1、SIGN#2、SIGN#3、SIGN#4)作成する。

【0034】なお、一つのフォーマットについての署名データを生成する際に、他のフォーマットで生成した署名データをも含めて署名対象とする方法としない方法とがある。前者の方法は、図4のフォーマット#1の例では、基礎情報DATA#1のほか、他の署名データSIGN#2、SIGN#3、SIGN#4を対象として署名データSIGN#1を作成する方法であり、後者の方法は、基礎情報DATA#1のみを署名対象として署名データSIGN#1を生成する方法である。

【0035】公開鍵証明書の基礎情報領域は、4つのパターンのいずれかにより表現されるので、ICカードに読み込ませる場合には、所定のフォーマット変換ルールに従って、必要なフォーマットに変換した後に読み込ませることになる。例えば公開鍵証明書の基礎情報がフォーマット#1で表現されたDATA#1であり、ICカードにおいてフォーマット#2で検証する場合は、基礎情報DATA#1をフォーマット#2に変換した基礎情報DATA#2内の署名データが、それに対応した署名データSIGN#2になっていることを確認する。フォーマット#2以外のフォーマットに変換する際も同様で

ある。

【0036】(第2実施形態)次に、第2の公開鍵証明書の発行方法の実施の形態を説明する。この方法を実施するためのシステム構成は、図1に示した公開鍵証明書サービスシステムとほぼ同様である。但し、この実施形態の公開鍵証明書サービスシステムは、認証局の構成が第1実施形態のサービスシステム1のものと異なる。本実施形態の認証局400は、図5に示した通り、通信制御部410、公開鍵証明書発行部420及び署名部430を有している。

【0037】公開鍵証明書発行部420は、公開鍵証明書発行の申請情報に基づいて複数のフォーマットに対応する基礎情報を生成する基礎情報生成部420aと、生成された基礎情報の各々をハッシュして複数のハッシュ値を生成するハッシュ部420bと、申請者で利用可能なフォーマットに対応する基礎情報と該基礎情報以外の基礎情報から生成したすべてのハッシュ値と上記署名データとを含めて公開鍵証明書を作成(発行)する発行部420cを含んで構成されるものである。

【0038】まず、この認証局400において、第1実施形態と同様、X509とEMVの互換性がある公開鍵証明書を発行する場合の動作を説明する。この実施形態では、X509(フォーマット#1)で表現された基礎情報をDATA#1、EMV(フォーマット#2)で表現された基礎情報をDATA#2とする。

【0039】基礎情報DATA#1は、EMVのみに必要な項目Bを別領域である拡張データとし、項目C、項目A、項目Bの順に並べて構築される。Cは、共通の項目である。基礎情報DATA#2は、X509のみに必要な項目Aを別領域である付属データとして、項目C、項目B、項目Aの順に並べて構築される。

【0040】認証局400では、まず、 $h(x)$ を一方方向性ハッシュ関数とし、ハッシュ値 $H1=h(C, A)$ 、ハッシュ値 $H2=h(C, B)$ を定義する。そして、これら2つのハッシュ値 $H1$ 、 $H2$ を連結した連結ハッシュ値を署名対象として認証局400の基本署名データを生成する。そして、基礎情報DATA#1、ハッシュ値 $H2$ 、基本署名データを含むX509公開鍵証明書を発行する。EMV公開鍵証明書については、基礎情報DATA#2、ハッシュ値 $H1$ 、基本署名データを含むものとして発行する。

【0041】具体的には、図6のフローチャートに示したような手順により、公開鍵証明書の発行がなされる。即ち、端末10から公開鍵証明書発行の申請情報を受け取ると(ステップS201)、公開鍵証明書発行部42は、各フォーマットに対応する項目(A、B、C)を生成するとともに、ハッシュ関数 $h(x)$ を用いてハッシュ値 $H1=h(C, A)$ 及び $H2=h(C, B)$ を求める(ステップS202)。

【0042】次に、ハッシュ値 $H1$ とハッシュ値 $H2$ と

を連結した連結ハッシュ値(H1|H2)を対象として署名データSIGNを生成する(ステップS203)。公開鍵証明書発行部42は、また、項目Cと項目Aを拡張データとし、項目Bとハッシュ値H2、基本署名データを含んだX509公開鍵証明書を発行し(ステップS204)、これを通信制御部410を通して端末10宛に送付する。

【0043】このX509公開鍵証明書をEMV公開鍵証明書に変換する場合は、EMVの基礎情報DATA#2を{C, B, A}、ハッシュ値H1をh(C, A)に変換する。一方、EMV公開鍵証明書をX509公開鍵証明書に変換する場合は、X509の基礎情報DATA#1を{C, A, B}、ハッシュ値H2をh(C, A)に変換する。

【0044】各公開鍵証明書の検証処理は、X509の場合は項目Cと項目Aからハッシュ値H1を求め、基本署名データSIGNが連結ハッシュ値(H1|H2)についての正しい署名データになっているかを確認することにより行う。一方、EMVの場合は、項目Cと項目Bからハッシュ値H2を求め、基本署名データSIGNが連結ハッシュ値(H1|H2)についての正しい署名データになっているかを確認することにより行う。

【0045】次に、第1実施形態の場合と同様、4通りのフォーマット(フォーマット#1、フォーマット#2、フォーマット#3、フォーマット#4)に対応できるようにした公開鍵証明書の例を説明する。図7は、この実施形態によるフォーマット変換の概念図である。

【0046】まず、フォーマット#1での基礎情報DATA#1と他の3つのフォーマットで表現された基礎情報(DATA#2、DATA#3、DATA#4)をハッシュ関数で求めた3つのハッシュ値(HASH#2、HASH#3、HASH#4)と、これらの3つのハッシュ値を連結した連結ハッシュ値を署名対象として生成した一つの基本署名データ(SIGN)とを用意する。第1実施形態の場合と同様に、公開鍵証明書の基礎情報領域は、4つのいずれかのパターンで表現されるので、ICカード20に読み込ませる場合には、フォーマット変換ルールに従って、必要なフォーマットに変換した後に読み込ませることが可能である。

【0047】フォーマットの変換は、次のようにして行うことができる。例えばフォーマット#1からフォーマット#2に変換する場合を考える。この場合は、まず、フォーマット#1の基礎情報DATA#1のハッシュ値HASH#1を作る。次に、基礎情報DATA#1を変換してフォーマット#2の基礎情報DATA#2を作る。変換前のハッシュ値HASH#2は不要となるので、捨てる。記憶領域に余裕がある場合は捨てなくとも良いが、基礎情報DATA#2とハッシュ値HASH#2とが整合していることの確認は必要である。フォーマット#2を検証する場合は、基礎情報DATA#2をハ

ッシュしてハッシュ値HASH#2を求め、HASH#1からHASH#4までを連結したものを署名対象として基本署名データSIGNを生成し、それが正しい署名データであるかどうかを確認する。

【0048】各ハッシュ値は、各々のフォーマットでの基礎情報をフォーマット変換できれば何時でも再生が可能なので、ICカード等のようなデバイスでは、検証処理後はそれらを保存する必要はなく、記憶領域を少なくすることができる。例えば図示のようにフォーマット#2の場合、検証処理後は、各ハッシュ値HASH#1、HASH#3、HASH#4は捨てることが可能である。この場合、他のフォーマットに変換する際に、フォーマット#1～フォーマット#4まで順番にフォーマット変換してHASH#1～HASH#4を再生することになる。

【0049】この実施形態による公開鍵証明書の発行方法では、第1実施形態が4つの署名データが必要となるのに対し、一つの基本署名データと3つのハッシュ値が必要となる。通常、署名データは、ハッシュ値よりかなり大きくなるので、この実施形態の方が、保存するデータ量は少なく済む。

【0050】また、第1実施形態及び第2実施形態では、認証局40が新規な構成要素を備えて構成される場合の例を説明したが、各実施形態の認証局40、400の機能をもった情報処理装置ないしシステムをネットワークN上に配置し、この情報処理装置ないしシステムを通じて上記機能ないし処理を実現しても良い。特に、情報処理装置ないしシステムをプロキシサーバで構成することで、外部から隠蔽された状態で公開鍵証明書を発行できるようになる。

【0051】

【実施例】次に、本発明の実施例を説明する。図8は、サーバ30とICカード20との間で、端末10を介して相互に公開鍵証明書を検証するとともに、正当な場合に各々の公開鍵を相手に渡して暗号通信を行えるようにする場合シーケンスチャートである。図8において、EMV-CERT#1は、ICカード20が保有する公開鍵#1の正当性を証明するための公開鍵証明書、X509-CERT#1は、端末10において利用可能なX509公開鍵証明書、X509-CERT#2はサーバ30が保有する公開鍵#2の正当性を証明するためのX509公開鍵証明書、EMV-CERT#2は、X509-CERT#2を変換したEMV公開鍵証明書である。

【0052】ICカード20を保有する利用者は、そのICカード20を端末10のリーダライタ14に装着する。ICカード20が装着されると、端末10は、ICカード20からEMV-CERT#1(EMVのフォーマットで基礎情報領域が生成されている)を受領し、これをデータ処理部11でX509-CERT#1に変換する(T301)。その後、検証処理部13でX509

ーCERT#1の検証処理を行い(T302)、そのX509-CERT#1が正当と判断できる場合は公開鍵#1を格納する(T303)。データ処理部11は、リーダライタ14を介してICカード20に検証終了信号を送信する。端末10は、また、ICカード20からX509-CERT#1をサーバ30に送信する要求を受領すると、端末10は、X509-CERT#1をサーバ30宛に送付する。

【0053】X509-CERT#1を受領したサーバ30は、検証処理部33でX509-CERT#1の検証処理を行う(S301)。正当と判断できる場合は、データ格納部34に公開鍵#1を格納する(S302)。また、データ格納部34に格納されているX509-CERT#2を端末宛10宛に送信する。サーバ30からX509-CERT#2を受領した端末10は、データ処理部11でX509-CERT#2をEMV-CERT#2に変換し(T304)、これをリーダライタ14を介してICカード20に送付する。

【0054】EMV-CERT#2を受領したICカード20は、検証処理部22でEMV-CERT#2の検証処理を行い(I301)、正当と判断できる場合は、データ格納部23に公開鍵#2を格納する(I302)。

【0055】この結果、ICカード20はサーバ30の公開鍵#2を格納し、一方、サーバ30はICカード20の公開鍵#1を格納することになり、これらの公開鍵を用いて相互に暗号通信を行う際に、相手側のデータの検証を行えるようになる。なお、フォーマットの変換に際して、標準的なフォーマットを一つ定め、それを經由する形で個別のフォーマットへの変換ルールを定義するようにすることが好ましい。このようにすることで、個別のフォーマットの数が多くなった場合にも容易に対応できるようになる。

【0056】

【発明の効果】以上の説明から明らかなように、本発明の公開鍵証明書によれば、複数のフォーマットを用いることが可能になるため、インフラ構築において汎用性の高いフォーマットを採用しつつICカード等のリソース

が小さいデバイスにおいても利用可能な簡易なフォーマットを採用することが可能となるため、インフラの重複開発や、ICカード等における公開鍵証明書によるリソースの浪費を防止できるようになる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る公開鍵証明書サービスシステムの構成図。

【図2】第1実施形態による公開鍵証明書の発行手順を示した図。

10 【図3】X509公開鍵証明書とEMV公開鍵証明書との間の項目の対応図。

【図4】第1実施形態による公開鍵証明書のフォーマット変換の概念図。

【図5】本発明の第2実施形態に係る公開鍵証明書サービスシステムの認証局の構成図。

【図6】第2実施形態による公開鍵証明書の発行手順を示した図。

【図7】第2実施形態による公開鍵証明書のフォーマット変換の概念図。

20 【図8】公開鍵証明書を検証する際のICカードと端末との間及び端末とサーバとの間の処理手順を示したシーケンスチャート。

【符号の説明】

1 公開鍵証明書サービスシステム

10 端末

11、21、31 データ処理部

12、32、41 通信制御部

13、22、33 検証処理部

14 リーダライタ

30 20 ICカード

23、34 データ格納部

30 サーバ

40 認証局

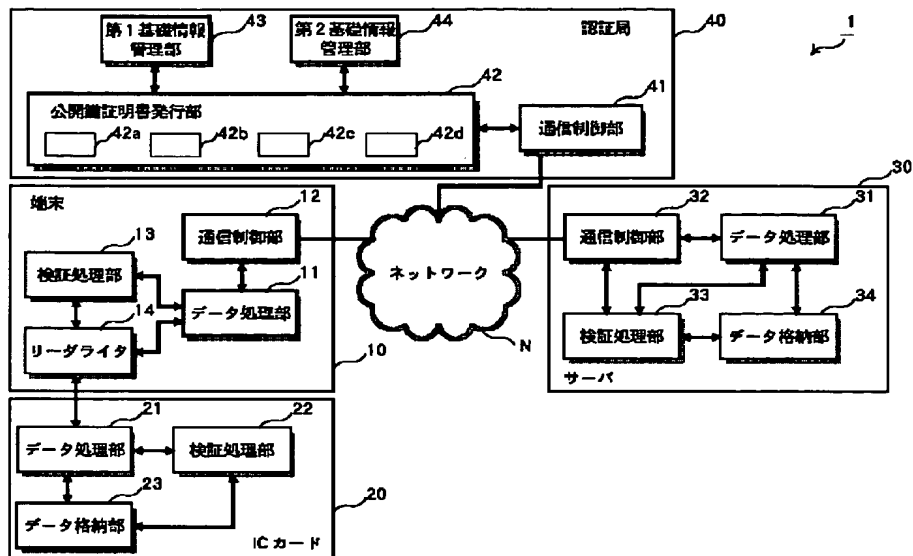
42 公開鍵証明書発行部

43 第1基礎情報管理部

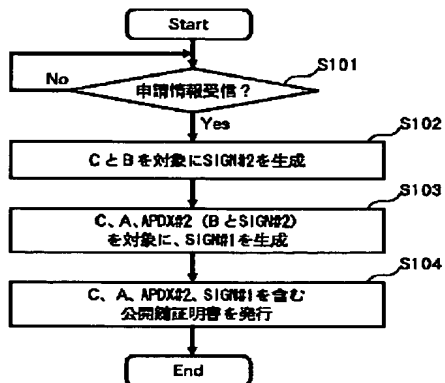
44 第2基礎情報管理部

Nネットワーク

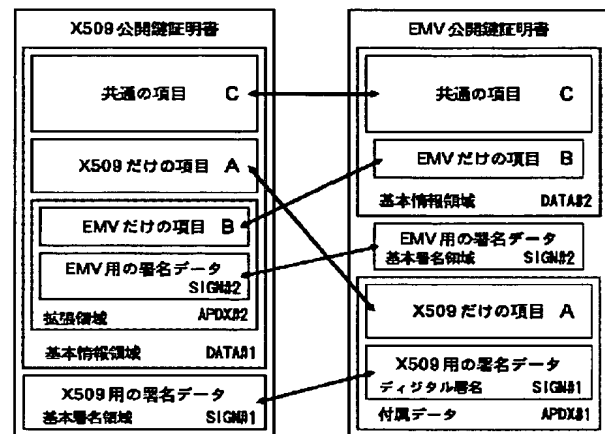
【図 1】



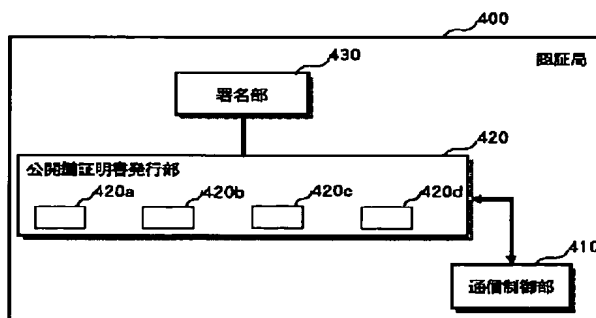
【図 2】



【図 3】

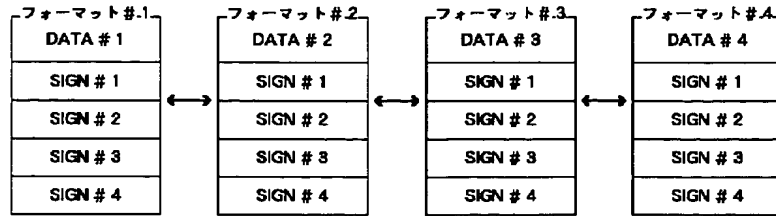


【図 5】

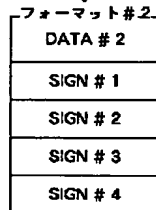


【図4】

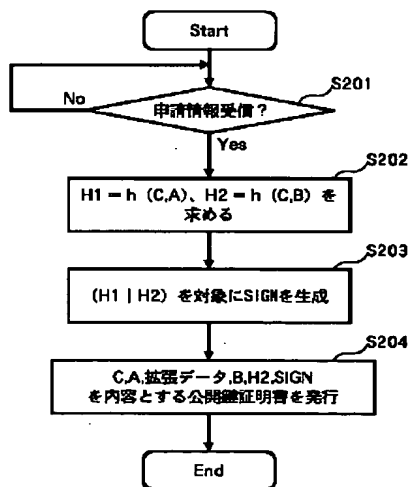
端末側



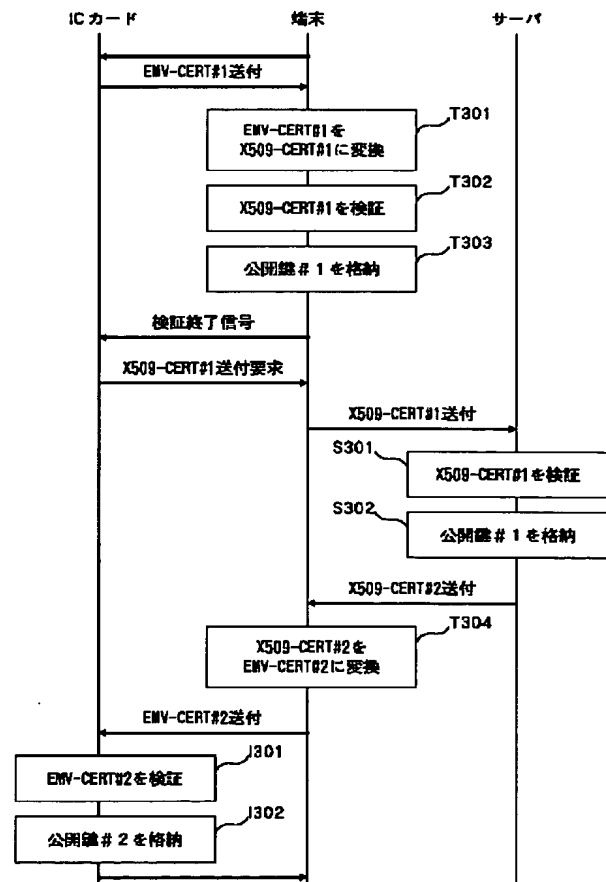
ICカード側



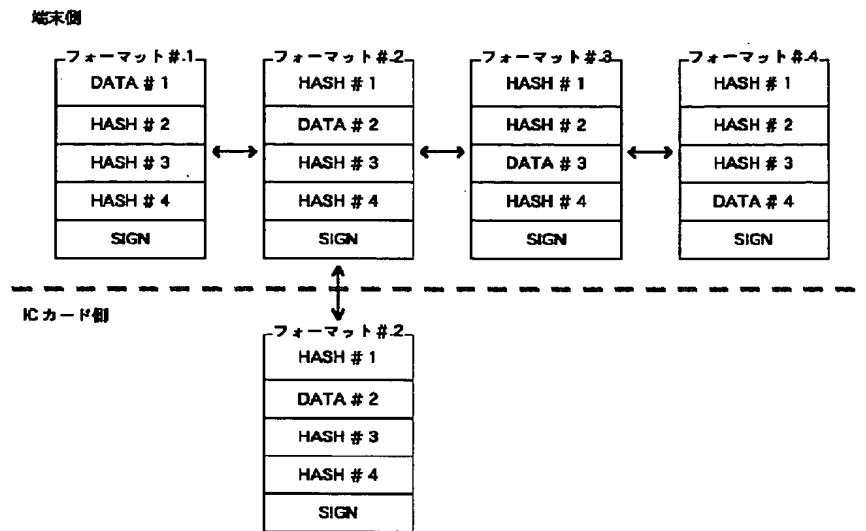
【図6】



【図8】



【図7】



フロントページの続き

(51) Int. Cl.⁷

H 0 4 L 9/32

識別記号

F I

H 0 4 L 9/00

テマコード* (参考)

6 7 5 D